connecting the future

Making Public Services Work for You with Your Digital Identity

Cabinet Office & The Rt Hon Darren Jones MP

10 March 2026

Response from The Payments Association

5 May 2026

Introduction

The Payments Association welcomes the opportunity to contribute to the consultation on 'Making Public Services Work for You with Your Digital Identity' from the Cabinet Office & The Rt Hon Darren Jones MP.

The community's response contained in this paper reflects views expressed by our members and industry experts recommended by them who have been interviewed and who are referenced below. As The Payment Association's membership includes a wide range of companies from across the payments value chain, and diverse viewpoints across all job roles, this response cannot and does not claim to fully represent the views of all members.

We are grateful to the contributors to this response, which has been drafted with feedback from our membership, with assistance from member Optimus Money. We would also like to express our thanks to the Cabinet Office for their continuing openness in these discussions. We hope it advances our collective efforts to ensure that the UK's payments industry continues to be progressive, world-leading, and secure, and effective at serving the needs of everyone who pays and gets paid.

Natasha Healy
Head of Projects
The Payments Association

Our members' views:

Overview

The Payments Association wishes to make two overarching observations:

First, the consultation does not ask directly about trust, despite trust being the most frequently raised concern in all three of The Payments Association's internal evidence sessions. The government should conduct dedicated public engagement on trust and privacy concerns as a matter of priority, and should be transparent about the data governance framework before the system is launched, not after.

Second, the terminology used throughout the consultation is inconsistent and likely to cause confusion. Terms such as 'digital identity', 'digital verification' and 'wallet' are used without a clear definition. The government should publish a clear glossary alongside any future consultation or implementation documentation. The absence of the words 'authentication' and 'verification' from the consultation document was specifically noted as a significant gap by members with technical expertise in identity systems.

Response to questions:

Part 1: Our Ambition

Q1: How are you responding to this consultation?
Responding on behalf of The Payments Association.

Q2: We would like to hear what people think about our proposals for the digital ID system. The core of the proposal is covered in part 1 of the consultation. All respondents will be shown questions about this part.

The remainder of the survey is split into five parts, numbered from 2 to 6, and then into chapters. You can answer questions from these based on your interests. Which parts of the consultation would you like to answer questions about?

The Payments Association would like to respond to every chapter of the consultation.

Q3: What do you think the main benefits will be, if any, for the government's new national digital ID system?

The Payments Association recognises the significant potential benefits of a well-implemented national digital ID system, subject to the important caveats detailed throughout this response.

The group identified the following potential benefits:

- Efficiency gains across public and private sector processes, particularly in onboarding, KYC refresh, and reducing abandonment rates in digital journeys.
- Improved financial inclusion for those who currently lack traditional proof of identity, enabling access to public services and financial products.
- A foundation for modernised public service delivery, including a streamlined 'one login' approach to government services, akin to interactions citizens already have with private sector providers such as online banking.

- Potential interoperability with open finance and smart data initiatives, future-proofing digital identity journeys.
- Support for right-to-work checks and tackling illegal working, where the current reliance on manual passport inspection is considered insufficient.
- Relevance to the emerging need for digital identity verification in the context of agentic commerce, where AI agents acting on behalf of individuals will require robust identity verification.

Some members believe that it is essential for digital ID to be available for KYC and KYB purposes for both people and businesses, and that this should be a government-led priority.

Q4: What do you think the main drawbacks will be, if any, for the government's new national digital ID system?

The group identified a number of significant drawbacks and risks which would need to be addressed for the system to deliver its stated ambitions:

- **Implementation costs:** The financial and operational costs of integration, staff training, process redesign, and ongoing monitoring will be very significant for businesses across all sectors.
- **Security risks:** The centralisation of identity data creates an obvious and high-value target for domestic and international threats.
  In the backdrop of Mythos and the rise of AI solutions, members identified significant cyber risks as having a digital identity system becomes a huge target for criminals and rogue state actors. Members questioned how the government would keep this data safe and ensure public trust to mitigate allegations that data has been stolen, etc.
  Members drew parallels with the collapse of the NHS National Programme for IT (NPfIT) in 2012, which cost £12 billion and failed in part due to inadequate identity verification and security architecture. Concerns were also raised about the current system's reliance on OneLogin, which has been acknowledged to have prior security vulnerabilities.
- **Trust deficit:** Trust and privacy concerns were flagged as potentially the most significant barrier to adoption. The consultation itself does not directly ask about trust, which members found notable. Fears of government overreach, data misuse, and 'Big Brother' surveillance were raised by multiple participants.
- **Lack of clarity:** There is insufficient detail in the consultation about who will build and operate the system, what the implementation phases are, and how accountability will be maintained across political cycles.
- **Risk to the private digital ID market:** If the government offers a free checker service with broad scope, this could undermine existing private sector digital verification providers and reduce consumer choice and market innovation.
- **Digital and financial exclusion risk:** Those who are most likely to struggle to obtain a digital ID, including people who lack traditional ID documents, elderly people, those with complex life circumstances, are also most likely to distrust the system, creating a paradox for inclusion goals.

Q5: One of the government's aims for the new national digital ID system is to make it easier for people to prove who they are. To what extent do you agree or disagree that the proposed system could help achieve the aim of making it easier for people to prove who they are?

Position: Somewhat Agree - with significant caveats.

The Payments Association broadly agrees that a digital ID system, if implemented correctly and securely, could make identity verification significantly easier for many people.

However, members were clear that agreement is conditional and heavily dependent on the quality of implementation. As noted by multiple participants in the evidence sessions, the answer to almost every question in this consultation is 'it depends on how it is done'.

Members specifically flagged that as currently described, there are insufficient security protocols in place to ensure the system could robustly prove identity without the risk of impersonation or fraud. Furthermore, the system risks making it harder, not easier, for digitally excluded and vulnerable individuals who already struggle with existing identity verification processes.

Q6: The government proposes to use the digital ID system to enable more modern, efficient and personalised public services. Which public services would you want the government to prioritise making faster or more efficient using the system?

The Payments Association recommends the government focus initially on core public service use cases where digital ID provides a clear, measurable improvement and where the risk of scope creep is minimised. Suggested priorities include:

- Right-to-work checks, where the current manual process is insufficient.
- Benefits access and entitlement verification, where identity barriers prevent vulnerable people from claiming support to which they are entitled.
- NHS and healthcare interactions, where fragmented systems currently create friction, while acknowledging the complexity of this integration, given the NHS's existing infrastructure challenges.
- Tax and HMRC interactions, including the current annual difficulty with accessing personal tax accounts and resetting credentials.

The government should resist pressure to extend the scope of the system beyond well-defined public service use cases in the early phases.

Chapter 2.1: Creating the Digital ID

Q7: Do you have any concerns about the impact of the national digital ID that are specific to your part of the UK?

The Payments Association has no specific concerns restricted to a particular region, but notes that any rollout must be mindful of the different legislative and regulatory environments in Scotland, Wales, and Northern Ireland, and must ensure that the system works equitably across all devolved nations. Members did not identify region-specific issues requiring distinct policy treatment at this stage.

Chapter 2.2: Storing, Managing and Using the Digital ID

Q8: Someone might wish to delete their own digital ID from their device. They will be able to do this at any time, and the process will be designed to be simple and quick. Are there any ethical factors the government should consider that relate to an individual deleting their digital ID?

Position: Yes.
The right to delete one's digital ID should be clearly protected and the process made simple. Ethical considerations include:

- The need to ensure deletion does not inadvertently cause hardship; for example, if the digital ID has been used as the sole means of accessing public benefits or services, deletion should not cause immediate exclusion.
- Clear communication to the individual about the downstream consequences of deletion across services.
- The process should mirror established data rights under UK GDPR, including the right to erasure under the Data Use and Access Act.

Q9: Under strictly controlled circumstances, the government may also have the power to revoke (i.e. cancel) someone's digital ID - for instance, if someone's digital ID has been identified as stolen or used fraudulently. This will be governed by robust processes.
Are there any ethical factors the government should consider that relate to revoking an individual's digital ID?

Position: Yes.
Members expressed strong views on this question. Revocation must be governed by a robust, transparent and apolitical framework. The key ethical considerations raised include:

- Revocation criteria must be objectively defined, legally grounded and clearly communicated, ensuring the process cannot be used for politically motivated purposes.
- There must be a balance between swift revocation where fraud or theft is identified, and protections against undue hardship, for example, where revocation could cause someone to lose access to employment, benefits, or healthcare.
- Parallels were drawn with the payment sector's 'additional time to make payment' rules under fraud provisions, where firms must be able to justify any delay with reference to clear criteria. A similar framework could be applicable here.
- Independent oversight of revocation decisions is essential to maintain public trust and prevent abuse.

Q10: Do you think people should be able to choose to store their national digital ID directly in holder services (sometimes known as 'digital wallets') other than the GOV.UK Wallet, that are certified to meet government standards?
Position: Yes.
Individuals should be able to store their digital ID in certified third-party digital wallets, consistent with their rights under the Data Protection Act 2018 and the Data Use and Access Act.

The Payments Association notes that this question presents an opportunity for regulated payment firms, including e-money institutions, to gain government accreditation to hold digital IDs alongside e-money.

The government should publish clear accreditation standards, regulatory requirements, and security frameworks for third-party wallets seeking to hold digital IDs. Interoperability between the GOV.UK Wallet and certified third-party wallets should be a design requirement, not an afterthought.

The consultation uses the term 'wallet' without definition, which caused confusion among members. Greater terminological clarity, including around authentication and verification, is needed throughout the consultation document and the final scheme design.

Chapter 3.1: Information Contained in the Digital ID

Q11: The national digital ID will include a person's full name, date of birth, nationality, and a biometric facial image (photo). What further information, if any, should the digital ID also include?

The Payments Association would support the inclusion of additional information only where it is proportionate, necessary, and accompanied by appropriate privacy safeguards. Members did not advocate for extensive additional data fields in the initial design.

A specific concern was raised regarding the inclusion of biometric facial images. If included, it is essential that any automated facial recognition or matching system is audited rigorously for algorithmic bias. Evidence of bias in facial recognition technology, particularly against people of colour, older people, and disabled individuals, is well documented, and the government must ensure that the system does not replicate or amplify these biases at the point of identity proofing or ongoing use.

Q12: To what extent do you agree or disagree with a legal requirement to inform the government of changes or errors within an appropriate timeframe?

Position: Agree - with questions about the reciprocal obligation of the government.
A legal requirement to inform the government of changes to personal information is reasonable and proportionate, drawing a parallel to existing legal requirements such as updating a driving licence following a name change.

However, members raised an important reciprocal question: how quickly will the government update the digital ID following a notification, and how will updated information flow across public services and to private sector organisations that have previously verified the individual's identity? Currently, the assumption is that verification is a 'one-and-done' point-in-time check; for the system to work as proposed, this model would need to change. The government should clarify the update propagation mechanism and associated timescales.

Chapter 3.2: Transforming Public Services

Q13:
Are there examples of any barriers or inefficiencies that prevent you (or people you support) from interacting with public services, that you think the digital ID system could help with?

Position: Yes.
The Payments Association recognises that many of the barriers to digital ID adoption mirror existing barriers to public service access. These include:

- Lack of traditional identity documents, particularly among homeless people, refugees, care leavers, and victims of domestic abuse; groups that often also face the most acute need for public services.
- Lack of digital access and skills, meaning those without smartphones, internet access, or digital confidence face compounding barriers.
- Trust and privacy concerns, as fear of data sharing or government surveillance may prevent uptake, particularly among communities that have historically had negative experiences with government institutions.
- Completing multiple identity verification processes across different services is a significant barrier, particularly for those with complex life circumstances or caring responsibilities.

The digital ID system could help to address some of these barriers, but only if supported by a well-resourced inclusion programme that reaches those who are most marginalised.

Q14: Have you ever faced issues with knowing which public services are available to you based on your circumstances or, if you support other people, have you faced similar issues when supporting them?

No comments.

Q15: Have you ever been unable to or had difficulty accessing a public service because you were unable to prove your identity or, if you support other people, have you faced similar issues when supporting them?

No comments.

Q16: To what extent do you agree or disagree with the adoption of a cross-service matching approach to public sector transformation?

Position: Somewhat Positive - with significant caveats.
The Payments Association recognises that cross-service matching is technically necessary to deliver many of the benefits set out in the consultation. Members were broadly positive about the potential to reduce bureaucratic duplication, particularly the need for individuals to update personal information separately across multiple government services. However, strong concerns were raised about implementation risk, auditability, and scope.

Specifically:

- Matching should be tightly limited to public sector services. Extension to private sector matching, without explicit individual consent, would raise serious surveillance and data privacy concerns.
- Citizens should be able to see which public services have access to their matched data, enabled through transparent audit logs and user-visible access records.
- The current fragmented state of UK government infrastructure as evidenced by the NHS's ongoing data interoperability challenges which raises serious questions about whether the necessary technical foundations are in place. The government should prioritise getting its internal infrastructure in order before expanding scope.

Q17: What ethical issues, if any, can you think of when designing a way to identify and match people across services?

The Payments Association identifies the following ethical issues:

- **Surveillance risk:** A unique identifier used across all government services, and potentially private sector services, could enable the government to build comprehensive profiles of citizens' activities, raising significant civil liberties concerns.
- **Scope creep:** The matching capability should be strictly limited to public sector use cases. Extending it to private sector interactions risks creating a surveillance infrastructure that exceeds the stated aims of the system.
- **Accountability across political cycles:** If the system becomes embedded in public service delivery, future governments must be bound by the same data use restrictions. The consultation does not address how such commitments would be enforced over time.
- **Algorithmic bias:** Automated matching of individuals across services introduces the risk of errors and biases that could disproportionately impact vulnerable groups.

Chapter 3.3: Utility in the Wider Economy

Q18: To what extent do you agree or disagree that the private sector and third parties should be able to use the digital ID alongside other options?

Position: Somewhat Agree.
The Payments Association broadly supports the use of the digital ID in the private sector, provided that it operates as one option within a competitive market of digital verification services, rather than becoming a de facto monopoly. Voluntary adoption and the coexistence of government and private sector alternatives are essential to maintain consumer choice, market diversity, and innovation.

The government must avoid scope creep that would allow the free government checker service to crowd out private digital verification providers. If the government offers a free or subsidised service that extends beyond core public sector use cases, this risks destroying the market for private identity verification services that have invested significantly in building compliant and effective solutions.

Chapter 3.4: Tackling Illegal Working

Q19: Are there any additional challenges not captured in the consultation that businesses would face in carrying out fully digital right-to-work checks for all new workers?

The Payments Association does not have a specific position on this question beyond noting the importance of clarity regarding which digital verification methods will be accepted for right-to-work checks. Right-to-work checks will need to be performed digitally, but the government's digital ID system should not be the only accepted route; existing Digital Identity Trust Framework (DITF) certified solutions should remain valid alternatives.

Chapter 4.1: Eligibility for the Digital ID

Q20: All British and Irish citizens, and foreign nationals with permission to be in the UK, who are above an agreed minimum age will be eligible for the national digital ID. Are there any other groups that should be included in eligibility?

The Payments Association notes a specific practical question raised by members: can individuals apply for the digital ID from abroad, or is an in-person presentation in the UK required? This is particularly relevant for British nationals living or working overseas who may need to access UK public services or prove their right to work on return to the UK. The government should clarify the eligibility process for non-resident citizens.

Q21: Which of the following ages do you think is most suitable to access the digital ID system from?

Position: 16 years old.
Given that the initial focus of the system is on public services and right-to-work checks, 16 years of age is the most practical starting point, aligning with the minimum working age.

Extending eligibility to younger ages would significantly increase the complexity of the system and should only be considered once the core system is functioning effectively. Birth registration is a separate and distinct matter from digital identity.

Chapter 4.2: Unlocking Access Across Society

Q22: Are you aware of any other barriers not captured in the consultation?

The Payments Association identifies the following barriers not adequately addressed in the consultation:

- **Low trust and fear of negative consequences:** The initial announcement of a mandatory digital ID generated significant public backlash. Despite the subsequent pivot to a voluntary model, the consultation does not address how the government plans to rebuild trust and overcome negative perceptions, particularly among communities most sceptical of government data collection.
- **Complex life circumstances**: People who frequently change personal details, such as those fleeing domestic abuse, individuals experiencing homelessness, or those with unstable living situations, face particular challenges in maintaining accurate identity records. This group is not adequately captured in the consultation's exclusion list.
- **Terminology and digital literacy**: The consultation's use of terms such as 'wallet' without definition, and the broader confusion around 'digital identity' versus 'digital verification', reflects a conceptual gap that will hinder public understanding and trust.

Q23: Is there any particular support not captured in the consultation or the Digital Inclusion Action Plan?

The Payments Association recommends the following additional support measures:

- Dedicated awareness and trust-building campaigns to address public concerns about surveillance, data misuse and government overreach, particularly targeting communities with historically low trust in government institutions.
- Partnerships with financial services providers, who have existing trusted relationships with customers and established KYC infrastructure that could support digital ID adoption in a way that feels familiar and trustworthy.
- Integration with the work of specialist charities and support organisations already operating digital inclusion programmes, for example, Project Nemo and disability organisations, to reach the most excluded individuals.
- Additional support for businesses of all sizes and competencies that may not have the resources or experience available to easily implement this new technology

Q24: Chapter 4.2 of the consultation includes a non-exhaustive list of those people who may benefit the most from additional support measures to ensure they are able to access the national digital ID. Are there any groups not included in the list that you believe could also be at risk of ID or digital exclusion?

Position: Yes.
In addition to the groups listed in the consultation, the Payments Association draws attention to:

- People in complex or unstable life circumstances (as noted above) who may have difficulty maintaining consistent identity records even where they have an initial digital ID.
- Armed forces personnel, who have distinct identity documentation and may face particular challenges if the system is not designed with their circumstances in mind.
- People with fluctuating mental health conditions, who may have periods in which they are unable to manage or maintain a digital ID, raising questions about access continuity and appropriate support.
- Some businesses may not have the resources or experience available to easily implement this new technology. Businesses of all sizes and competencies must be considered to ensure are able to access digital ID and reap the potential benefits.

Chapter 4.3: Commitment to Supporting Inclusion

Q25: What kind of support should be made available to people who do not have a digital device (like a smartphone or tablet) to enable them to create and access the digital ID?

The Payments Association supports all three options listed in the consultation (dedicated local help, trusted individual support, and skills programmes) and recommends they be pursued in combination.

In addition, members suggest:

- Awareness campaigns through trusted community intermediaries, such as GPs, post offices, libraries, and community centres, to ensure people without digital access are informed about the system and available support.
- Formal partnerships with charities already delivering digital inclusion support, such as Project Nemo, to leverage existing infrastructure and trusted relationships.

Chapter 4.4: Accessibility

Q26: Can you suggest any specific organisations or types of organisations which the government should engage with?

The Payments Association recommends the government engage with the following types of organisations:

- Disability and accessibility organisations, which were notably absent from the consultation's engagement plans.
- Financial inclusion charities with existing digital inclusion programmes, including Project Nemo, with which the Payments Association already has an established working relationship.
- Civil society organisations supporting homeless people, refugees, domestic abuse survivors, care leavers, and other groups at high risk of identity exclusion.
- Regulated financial services firms, including banks and payment institutions, which have extensive experience in designing accessible identity verification journeys and in reaching financially excluded customers.

Chapter 4.5: Alternative Access Routes

Q27: What do you think are the most important barriers for government to address when designing alternative access routes for the national digital ID?

The Payments Association identifies the following as the most important barriers for alternative access route design:

- Ensuring alternative routes are as secure as the primary digital route, to prevent exploitation by fraudulent actors.
- Avoiding two-tiered access in which those using alternative routes receive a lower quality or less reliable digital ID, which could undermine their ability to access services on an equal basis.
- Building in flexibility to accommodate people whose circumstances change, for example, those who gain access to a device after initially using an alternative route.

Chapter 5.1: Data Protection and Privacy

Q28: Are there any additional measures, beyond the principles and standards set out in the consultation, that we should consider to further protect user data?

No comments.

Chapter 5.2: Securing the National Digital ID Scheme

Q29: Are there any additional security safeguards to those named above that should be considered in relation to the national digital ID system?

Position: Yes.
The Payments Association recommends the following additional data protection measures, informed by members' experience in financial services:

- Strong authentication and step-up controls for sensitive actions involving the digital ID.
- Encryption of data both in transit and at rest, with clear and publicly available rules on data retention limits and deletion timescales.
- Transparency logs and user-visible access records, enabling citizens to see which government services have accessed their data and when.
- The Payments Association notes that the primary empowering legislation, the Data Use and Access Act 2025, builds on the framework established by open banking and the Open Banking Limited (OBL) standards. This means the regulatory impact assessment for the Act effectively requires the digital ID system to meet, at a minimum, the security standards that the payments industry already applies in its day-to-day operations. The government should make this explicit in its implementation framework.

In addition to the measures noted above under data protection, the Payments Association recommends:

- Security standards for the digital ID system must meet or exceed the standards currently applied in financial services, including multi-factor authentication, biometric verification, and robust access controls.
- The consultation's own documentation appears to categorise the system as 'medium' security under Cabinet Office Government Protective Marking definitions, despite ministerial statements claiming it will meet the highest banking standards. This inconsistency must be resolved, and the final system should be explicitly certified to the highest available standards.
- The historic failure of the NHS NPfIT, which collapsed after costing £12 billion due to inadequate identity verification and access controls, should serve as a critical case study in what to avoid.
- The government should publish a clear security architecture and subject it to independent audit before launch, with ongoing annual reviews.

Chapter 5.3: Fraud as a National Challenge

Q30: To make sure everyone can access and use the national digital ID, the application process will need to offer alternative routes and additional support for those who need them. We want to ensure these alternative access routes are secure. What do you think are the most important factors we need to consider in order to achieve this?

The Payments Association recommends the following factors be prioritised:

- Alternative routes must be subject to the same rigorous identity proofing as the primary digital route, even if the process is delivered through different channels.
- Fraud controls for alternative access routes should be developed in coordination with the Home Office, the new Online Crime Centre, and law enforcement agencies, given that the fraud strategy and associated powers are still being operationalised.

- The government should monitor alternative access route usage patterns for anomalies that may indicate fraudulent exploitation, using the same data-driven fraud detection approaches already deployed in the payments sector.

Q31: What are the most important factors to consider when ensuring alternative access routes are not misused by fraudulent actors?

The Payments Association recommends:

- Clear and consistently applied identity proofing standards across all access routes, with no route offering a lower standard of verification.
- Signposting to law enforcement and the Online Crime Centre as the primary mechanism for addressing evolving fraud risks, with the digital ID framework designed to be updated dynamically as fraud tactics change.
- Drawing on the experience of regulated financial services firms, which have developed sophisticated approaches to detecting and preventing identity fraud at the point of onboarding and throughout the customer lifecycle.

Chapter 5.4: Ensuring Strong Oversight and Governance

Q32: What additional oversight mechanisms, if any, would help you to have trust in the national digital ID system?

The Payments Association regards robust and genuinely independent oversight as the single most important factor in building public and industry trust in the national digital ID system.

Members raised the following specific recommendations:

- An independent oversight body, distinct from the Cabinet Office and insulated from political interference, should be established with statutory powers to scrutinise the operation of the digital ID system.
- The oversight framework must be designed to be durable across political cycles. Accountability should not depend on the continued goodwill of any particular administration.
- If private sector organisations are involved in any aspect of oversight, their independence must be clearly policed and demonstrably free from commercial conflicts of interest.
- 'Four eyes' principles, requiring dual authorisation for sensitive actions such as revocation decisions or data sharing authorisations, should be built into the governance framework.
- The question of who holds ultimate accountability when things go wrong is not answered in the consultation and must be addressed before the system goes live.

Q33: What measures do you think should be in place to help you feel confident in resolving any issues with your national digital ID?

The Payments Association recommends:

- A clear, accessible, and well-publicised complaints and redress process, with defined timescales for resolution.
- A named accountable authority responsible for resolving disputes, with the power to compel government departments to act swiftly where a citizen's access to services has been affected.
- Transparency reporting on the number and nature of issues reported, actions taken, and resolution times, published annually.

Part 6: Wider Summary of Impacts

Q34: Do you think there are any other benefits for businesses from introducing the national digital ID system that have not been considered?

Position: Yes.
The Payments Association identifies the following additional business benefits:

- Reduced onboarding friction and lower abandonment rates in digital customer journeys, particularly in financial services, where KYC requirements create significant friction.
- More efficient KYC refresh and re-verification processes, reducing the cost of compliance over the customer lifecycle.
- Potential for the digital ID to become interoperable with open finance and smart data initiatives, creating a single, trusted identity layer across a range of regulated sectors.
- Support for the development of agentic commerce, where AI agents acting on behalf of individuals will require robust, standardised identity verification that neither current systems nor private sector alternatives can yet provide at scale.

Q35: Do you think there are any other costs to businesses from introducing the national digital ID system that have not been considered?

Position: Yes.
The Payments Association identifies the following additional business costs:

- Integration and API development costs, which will vary significantly by organisational size but will be material for all businesses required to accept the digital ID.
- Staff training and process redesign costs, which are likely to be ongoing as the system evolves.
- Ongoing monitoring and governance costs, which will be necessary to maintain compliance with the system's security and data protection requirements.
- Market disruption risk for private digital verification providers, which may face significant loss of revenue if the government's free checker service expands beyond its stated initial scope.

Q36: Do you think there are any other benefits for households from introducing the national digital ID system that have not been considered?

No comments.

Q37: Do you think there are any other costs to households from introducing the national digital ID system that have not been considered?

No comments.

Q38: Do you believe there are any other wider impacts from introducing the national digital ID system that have not been considered?

Position: Yes.
The Payments Association wishes to draw attention to the following wider impacts:

- Impact on trust in digital identity more broadly: If the government's digital ID system fails, is breached, or is perceived as intrusive, this will damage public trust not only in the government's scheme but in private digital identity verification services across the market. The stakes are therefore much higher than the consultation acknowledges.
- Sovereign and geopolitical considerations: The question of whether the technical infrastructure underlying the digital ID should be provided by domestic or allied-

nation companies, or whether it would involve major US technology companies such as Palantir, Google, or Apple, raises important questions of digital sovereignty that the consultation does not address. Members drew parallels with European discussions about tech sovereignty in the context of digital passports and border control.

- Agentic AI and machine-to-machine identity: As AI agents increasingly act on behalf of individuals in commercial and public sector contexts, the need for robust digital identity infrastructure extends beyond human identity verification. The digital ID framework should be designed with this future use case in mind.

Q39: Is there anything else not covered by these questions that you wish to share with us as part of this consultation?

The Payments Association wishes to make two overarching observations:

First, the consultation does not ask directly about trust, despite trust being the most frequently raised concern in all three of The Payments Association's internal evidence sessions. The government should conduct dedicated public engagement on trust and privacy concerns as a matter of priority, and should be transparent about the data governance framework before the system is launched, not after.

Second, the terminology used throughout the consultation is inconsistent and likely to cause confusion. Terms such as 'digital identity', 'digital verification' and 'wallet' are used without a clear definition. The government should publish a clear glossary alongside any future consultation or implementation documentation. The absence of the words 'authentication' and 'verification' from the consultation document was specifically noted as a significant gap by members with technical expertise in identity systems.

About The Payments Association

The Payments Association is for payments institutions, big & small. We help our members navigate a complex regulatory environment and facilitate profitable business partnerships.

Our purpose is to empower the most influential community in payments, where the connections, collaboration and learning shape an industry that works for all.

We operate as an independent representative for the industry and its interests, and drive collaboration within the payments sector to bring about meaningful change and innovation. We work closely with industry stakeholders such as the Bank of England, the FCA/PSR, HM Treasury, Pay.UK, UK Finance and Innovate Finance.

Through our comprehensive programme of activities for members and with guidance from an independent Advisory Board of leading payments experts, we facilitate the connections and build the bridges that join the ecosystem together and make it stronger.

These activities include a programme of digital and face-to-face events including our annual PAY360 and FC360 conferences, our PAY360 Awards dinner, PA@The City, CEO round tables, webinars, working group events and training activities.

We run eight stakeholder working groups: Cross-Border, Digital Currencies, ESG, Financial Crime, Financial Inclusion, Merchant Payments, Open Banking and Regulatory. The volunteers within these groups represent the collective view of The Payments Association members at industry-critical moments and work together to drive innovation in these areas.

Our Payments Intelligence team and our working groups aim to produce regular thought-leadership for our membership and beyond. These include data-driven reports, articles, video interviews and podcasts. We also undertake policy development and government relations activities aiming at informing and influencing important stakeholders to enable a prosperous, impactful and secure payments ecosystem.

See www.thepaymentsassociation.org for more information.

Contact natasha.healy@thepaymentsassociation.org for assistance.